Comcast подозревают в хакерских методах

Старые преданья начинались и заканчивались кровью.

Разное

Никогда не пробуйте читать что-нибудь научно-популярное, с претензией на достоверность, в онлайне. Дурная привычка - неизбежно захочется выделить несколько слов, дернуть их мышкой на google... И быстро убедиться, что автор, мягко говоря, многого не договаривает.

Полигоном послужила Бушковская Неизвестная Азия. Какой факт не потянешь, из тех простых, что будут на первой-пятой ссылке раздачи поисковика, - выходит искажение, натяжка, ошибка... Вроде бы и мелочь, но уже совершенно иное впечатление от книги, захочешь - не поверишь. А жаль, концепция красивая и правдоподобная.

Бедные авторы, с внедрением ШПД и электронных книг в быт им предстоит узнать много нового о своем творчестве. Отчасти похожая история была полтора столетия назад, когда фотография, изобретенная Дагером в 1839, грозила художникам безработицей. Далеко не бесталанный Поль Деларош представил во французскую Академию наук записку с сакраментальными словами "Живопись умерла с этого дня".

Слухи о смерти оказались, конечно, преувеличенными. Но многим труженикам кисти и в самом деле пришлось менять работу. Оставшиеся поставили во главу угла лозунг "автор так видит" и продолжили творчество. Интересно, как будут выкручиваться из противостояния с Сетью нынешние писатели-портретистыдокументалисты.

Поднял фото из своего архива. Нет, это не провайдерские ужастики - идет обычный ремонт здания.




Забавно только, что это самый центр Екатеринбурга, в 30-ти шагах от входа в арбитражный суд Свердловской области. Симпатичный домик на заднем фоне - резиденция губернатора, слева виден памятник основателям города.

Для начала немного ссылок по "сотовой" теме.

Организацию очередной небольшой сенсации в рамках Mobile World Congress в испанской Барселоне взяли на себя представители Google. Итоги обработки статистики запросов показали, что владельцы Apple iPhone используют поисковик Google в 50 раз чаще, чем покупатели любого другого мобильного гаджета.

Разница большая, и сперва в цифру просто не поверили. Но все подтвердилось, теперь конкурентам Apple придется искать объяснение свершившемуся факту. На мой взгляд, впрочем, тут нет чуда - коммуникатор с большим экраном впервые стал массовым, и использование любого подобного инструмента скорее как компьютера (а не телефона), стало статистически заметно.

Думать будут и с другой стороны сервиса. Нет сомнений, что остальные производители выпустят нечто айфоновидное, и буквально через несколько лет количество запросов "с телефонов" превысит компьютерные.

И это лишь демонстрация небольшого фрагмента картины нового сетевого мира, который ждет за переломом следующих трех-пяти лет. **Нужен "тонкий клиент", идеально приспособленный для работы в интернет? Вот прототип, получите и распишитесь.** Культовый, массовый, мобильный, оснащенный видеокамерой и приличным звуком.

Современному коммуникатору не хватает лишь полноразмерной клавиатуры, большого гибкого экрана и более емких (вероятно химических) элементов питания. Причем все уже изобретено,

внедрение в быт вопрос технологий и маркетинга.

Кошмарный сон для производителей компьютеров начинает сбываться. Не многим требуется колоссальная производительность четырехядерных интелов. Вернее, в ширпотребной нише она никому не нужна. Геймеры "мигрируют" на приставки, они уже дадут фору большинству ПК. Для повседневной домашней работы и серфинга телефон + телевизор (он же монитор) будут куда удобнее и дешевле.

Стационарная телефония обречена, похоронить ее смогут ОПСОСы и без сторонней помощи. Но когда у каждого в кармане появится включенный в интернет компьютер, со всеми вытекающими email-icq-sip-skype-foto-video-paypal-webmoney возможностями, неизбежно произойдет коммуникационный взрыв. Осколками порвет на куски всю отрасль.

Провайдеры по прежнему, в сравнении с 3G-4G-, смогут дать пользователю большую полосу и за меньшие деньги, но даже это не сможет переключить многих "мобильщиков" на стационарный канал. Помешает лень, привычка, незначительность ценовой разницы. Полного вытеснения, полагаю, не произойдет, но до 30% доля мобильных технологий доступа дотянется.

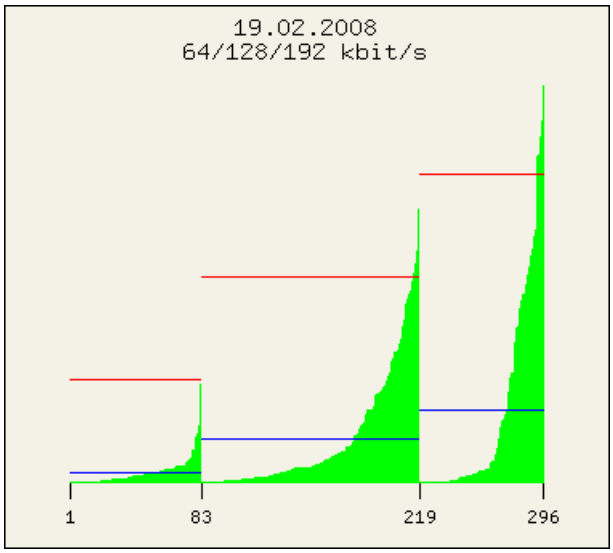
Лишь поставщикам контента и услуг не надо искать место в новом мире. Они уже готовы, и более того - выступают тем локомотивом, который толкает на рынок все более и более интеллектуальные сотовые трубки.

Для закрепления эффекта можно посмотреть еще один интересный отчет с Mobile World Congress 2008.

PS. Полагаю, ОПСОСы очень хорошо понимают перспективы рынка. И торопятся, МТС намерена в текущем году развернуть коммерческую сеть 3G в Красноярске и Норильске. Всего в развитие 3G МТС инвестирует около $1,55 млрд к 2011 г. "Вымпелком" и "Мегафон" пока не называют регионы развертывания 3G, но и у них существуют подобные планы.

PPS. На этом фоне строительство беспроводных сетей городского масштаба выглядит бледно: Питерский WiMAX получился медленным и дорогим. Подключение на скорости 512 кб/с без ограничения трафика обойдется в 10 тыс. руб. в месяц. Это фактически ограничительная цена, установленная не для извлечения максимальной прибыли, а скорее просто защищающая несовершенную сеть от большого количества абонентов.

Совершенно живая аналитика анлимитов.



Графики показывают среднюю за сутки скорость (Y) потребления внешнего трафика клиентами (X), которые используют тарифы БДС-64/128/192 от ТензорТелеком (Ярославль).

Только вот недавно говорили о неблизких перспективах IPv6, но уже в феврале МТУ получила префиксы, которые, возможно, уже скоро будет раздавать. Список Список участников, в котором можно найти ru.mtu, ZAO MTU-Intel, 20080213 2a02:0028::/32
Вполне вероятно, потянуться и другие крупные игроки.

По информации с форума, у Сибирьтелекома действуют нормативы на использование телефонных кабелей под DSL. Выделяется не более 10 пар в 100 парном кабеле и не более трех в 10-ти парном. Если число превышено - не подключают, "нет технической возможности".

Недавно параметры были изменены на "не более 18 пар на 100-парнике", что не замедлило сказаться на качестве работы всех абонентов. Днем как будто нормально, вечером в 6-8 часов параметры линии плывут, у многих связь начинает рваться. Помогает принудительная установка более медленного профиля.

Так как данная ситуация резко снижает инвестиционную привлекательность технологии АДСЛ, публичные данные найти сложно. Единственное, что попалось - особенности развертывания асимметричных цифровых абонентских линий в Украине, что вполне применимо и для России.

Способ борьбы с проблемой существует, он давно опробован Дойчтелекомом. Технология называется FTTC, Fiber To The Curb — оптоволокно до активного шкафа (выноса от АТС в жилой дом или, хотя бы, квартал).

Именно такую программу запустил на прошлой неделе МГТС под ADSL2+, что, по идее, должно в четыре раза увеличить скорость. Инвестиции в проект составят до $100 млн, т.е. **около $300 на абонента**. Не дешево выходит "догонять" домашние Ethernet-сети. И не быстро - строительство выносов займет года три, не меньше. Можно даже сказать, что МГТС опять опоздала - для сегодняшней конкурентной борьбы надо было начинать процесс еще в 2005 году.

Забавная цитата - *Если уж МГТС и тянет оптоволокно до каждого дома, то имело бы смысл доводить интернет до конечного потребителя по технологии Ethernet* - считает эксперт CNews Analythics Игорь Королев. Предложение, конечно, недостаточно квалифицированное (мягко говоря), но вот потеря журналистами веры в будущее АДСЛ - весьма отрадный факт.

Креатив, 90 серия VoiceCom, компании Натекс Нетворкс.

Ссылки в один абзац:

Дело о сериальных маньяках. Компьютерра посвятила последний номер января теме несанкционированного распространения популярных зарубежных сериалов в Рунете.

В Екатеринбурге 16 феврался прошел запуск цифрового телевидения Свердловской области. Сигнал будет передаваться в формате телевидения DVB-T с кодированием MPEG 4. Аналоговое вещание в регионе сохранится до 2015 года.

Адвокат А.С. Титов прокомментировал новые меры Правительства по пополнению резерва универсального обслуживания.

РФ стала мировым лидером в распространении компьютерных вирусов. Вот уж где не стоит гнаться за первым местом.

ФНС выдвинула миллиардные налоговые претензии Ростелекому. В частности, сообщается, что сумма предъявленных претензий за 2004 - 2006 гг. составляет более 1,8 млрд рублей, из которых 0,4 млрд – штрафы и пени.

Обновление в разделах:

- Пополнение в разделе "Фотографии сетевого оборудования": беспроводные адаптеры с поддержкой черновика стандарта 802.11n: TrendNet TEW-623P1 и TrendNet TEW-624UB ;
- На **карте городов** Prov.Nag.ru теперь 1046 провайдеров. Если кто-то желает дополнить информацию по городу или провайдеру - прошу писать на prov@nag.ru.
- В разделе shop.nag.ru появились новые разделы - оборудование для сетей КТВ и модули SFP CWDM .

Кроме того, существенно, до $2200, снижена цена на **Cisco 3745**.

Наиболее интересные темы форума (TOP-5):

- Ну, это уже ни в какие ворота...;
- Предсказуемое развитие, МГТС ставит "активные шкафы" для ADSL;
- Трансгелеком. Строительство розничной сети в регионах., События, факты, комментарии;
- Свитчи D-Link (электролиты в источниках питания);
- Линк на 25 км, желаемая скорость до 5 мбит.

Comcast подозревают в хакерских методах борьбы с пользователями

Comcast - второй по величине провайдер доступа к глобальной сети в США. Во многих районах страны это единственный, или один из двух, поставщик услуг кабельного телевидения и широкополосного интернета. Ориентировочно в мае 2007 года Comcast произвел модернизацию своего оборудования и программного обеспечения, после чего в прессе начали мелькать сообщения о появлении у некоторых клиентов определенных проблем со связью. Наиболее известными стали случаи перебоев с подключением к P2P-сетям BitTorrent, хотя сообщения и о других проблемах не были редкостью. По косвенным признакам некоторые специалисты предположили, что Comcast использует оборудование компании Sandvine, пишет Electronic Frontier Foundation (EFF).

Первые сообщения о трудностях подписчиков Comcast при получении данных из сетей BitTorrent появились на форумах и в блогах еще в мае текущего года. Обнаружение отдельными продвинутыми пользователями пакетов TCP RST, инициирующим преждевременный обрыв связи, привело к подозрениям о причастности к возникшим проблемам самого оператора Comcast.

Представители EFF попытались получить комментарии по этому поводу в Comcast и получили ответ в том смысле, что кабельный гигант, разумеется, управляет движением трафика в своих сетях, что могло в исключительно редких случаях помешать отдельным подписчикам, но ни о каком преднамеренном блокировании трафика BitTorrent речи быть не может.

В EFF этим ответом не удовлетворились и продолжили сбор информации, а также самостоятельное изучение пакетов при тестовой попытке скачать файл из сетей BitTorrent. Аналогичные опыты, по всей видимости, проводила и Associated Press (AP), причем выводы обоих информационных изданий совпали: RST пакеты действительно появлялись неизвестно откуда и становились причиной обрыва связи.

Во время тестирования исследователи из EFF использовали сниффер Wireshark, позволяющий отследить и оценить отдельные пакеты. Приемником данных выступало подключение через Comcast, а отправителем - некий хост в другой сети. Было обнаружено, что время от времени одна из сторон получает 3-5 RST-пакетов, обозначающих предложение разорвать связь, хотя другая сторона такие пакеты не отправляла. Т.е. это выглядело так, словно кто-то специально генерировал такие ложные пакеты, с подделкой идентификационных данных (например, IP-адрес) отправителя или получателя, и пытался "изобразить" ситуацию, как желание одной из сторон разорвать соединение.

Анализ ситуации показывает, что, скорее всего, ложные пакеты генерируются в сети Comcast, поскольку аналогичные проверки с использованием подключений от других провайдеров (было проверено более десяти разных подключений) таких проблем не выявили. Единственное внятное объяснение возникшей ситуации заключается в намеренной подделке пакетов со стороны Comcast, чтобы препятствовать прохождению трафика из определенных сетей.

Первые исследования показали, что Comcast создает помехи для определенного набора протоколов, а не для всего трафика TCP/IP в целом. В ходе тестирования специалисты EEF выявили вмешательство в сессии BitTorrent, Gnutella, а также Lotus Notes, используемой многими компаниями для обмена электронной почтой и скачивания файлов, выложенных для общего доступа. Правда, после первого шума, поднятого общественностью, проблемы с Lotus Notes вроде бы прекратились. Одна из компаний сообщала, что наблюдает проблемы с обеспечением нормальной работы удаленных рабочих столов для Windows, но спустя некоторое время заявила, что проблема исчезла сама собой. И хотя в последнем случае не было явной регистрации фальшивых пакетов, проблема исчезла тогда же, когда перестали жаловаться пользователи Lotus Notes, что лишний раз подтверждает наличие общей причины и весьма вероятную причастность Comcast.

EFF также получала неподтвержденные документально сведения о странных обрывах коннекта при закачивании средних и больших по объемам файлов по протоколам FTP и HTTP. Проверка исследователями EFF вроде бы показала наличие таких проблем, но уверенно получить их повторения не удалось и поэтому говорить о причастности к таким дисконнектам Comcast пока нельзя.

Конечно, для составления полной картины вероятной негативной деятельности Comcast данных пока недостаточно, но первые выводы сделать уже можно.

Сам кабельный гигант пытался замаскировать существующие проблемы, объясняя их небольшими задержками для незначительного количества сеансов связи, вызванными исключительно процессами управления сетью. И технически, и метафорически такая характеристика положения дел неполна и откровенно вводит конечного потребителя в заблуждение.

Подделка пакетов TCP RST имеет сложные и не всегда очевидные последствия. На низком уровне RST-пакеты обрывают те сеансы связи, для которых они предназначены. Но практические, видимые подписчиком Comcast, трудности в значительной степени зависят от того, какой высокоуровневый (Gnutella, BitTorrent, Lotus Notes и т.д.) протокол для какого программного обеспечения был использован.

Наиболее очевидное последствие - невозможность штатного функционирования программного обеспечения подписчика. К примеру, клиент Comcast не сможет поделиться информацией через сеть BitTorrent, поскольку ее просто никто не сумеет от него скачать.

В случае типичного узла Gnutella, фальшивые RST-пакеты будут блокировать возможность обнаружения и установки связи с другими узлами этой сети. Сеансы связи Gnutella могут инициироваться не только самим узлом, но и по запросу "снаружи", от других узлов сети. Типичным поведением активизированного узла является перебор доступных ранее других узлов по списку из кэша, в попытке восстановить какую-нибудь связь. Справедливо и обратное правило: "снаружи" другие узлы могут постоянно пытаться установить связь с узлом клиента Comcast, поскольку его адрес записан в их кэше или один из узлов сообщает остальным, что "видит" его в режиме онлайн.

Специалисты EFF на уровне пакетов наблюдали, как блокируются попытки соединения из внешних сетей с узлом Gnutella пользователя Comcast. На практике, это будет обозначать гораздо большее время, необходимое для организации гарантированно надежного соединения. А значит и уменьшает эффективность взаимодействия узлов Gnutella, находящихся в пределах инфраструктуры Comcast. Что обозначает масштабное воздействие на всю структуру сети Gnutella целиком.

Следует отметить, что в ходе тестирования специалисты EFF не заметили влияния подделки RST-пакетов на поиск информации или обмен трафиком в сети Gnutella. Речь идет о влиянии на процесс поиска узлов и первоначальной активации сеанса связи. Поэтому трудно сказать, какое количество конечных пользователей Gnutella испытывает реальные трудности из-за сомнительной деятельности Comcast. Но можно предположить, что человек, впервые запустивший Gnutella и безрезультатно проведший некоторое время в попытке соединения с другими узлами, может сделать вывод о неэффективности этой сети.

Разумеется, невозможность скачать файл через соединение BitTorrent и проблемы организации сеанса связи с узлом Gnutella нельзя объяснять некоторой задержкой трафика. Речь, несомненно, идет именно о блокировке. Поэтому, описывая причину проблем как "задержку" трафика, Comcast лукавит. Скорее, дело обстоит с точностью до наоборот: в некоторых случаях блокировка трафика выглядит как задержка. Например, если то специализированное ПО, что использует Comcast, работает дискретно во времени, настойчивый подписчик все-таки может дождаться начала соединения, и будет думать, что имела место именно задержка. Или если пользователь BitTorrent за пределами сети Comcast скачивает файл у подписчика кабельного гиганта и еще у кого-то в другом месте, то после обрыва связи с первым, все-таки докачает файл от второго, хоть и намного медленнее. Т.е. получит результат с задержкой. И также будет считать, что это была не блокировка.

Одной из главных претензий к Comcast во всей этой истории является факт подделки идентификаторов пакета, т.е. действия более приличествующие злоумышленникам, нежели одному из крупнейших операторов связи в стране. В этом смысле Comcast поступает намного хуже, чем, если бы уменьшал полосу пропускания для определенных видов трафика или блокировал определенные порты.

На первый взгляд Comcast обманывает всего лишь компьютеры, а не людей, но пользователи, получая неверную информацию, вынуждены искать пути решения, неизвестно откуда возникшей, проблемы. Это также обозначает, что программисты не могут опереться на работу стандартных протоколов, чтобы гарантировать правильную работу своих программ. Ведь в алгоритм программного кода придется каким-то образом закладывать вероятность того факта, что пришедший RST-пакет является фальшивым. Другими словами, интернет-провайдер может стать настоящим непредсказуемым фактором, о котором разработчикам ПО придется теперь помнить постоянно.

Кроме того, поведение Comcast угрожает дальнейшему развитию новых сетевых технологий, поскольку подрывает сами основы свободы и непрерывности интернета. Если изначально любой программист, будь он сотрудником могущественной корпорации или частным разработчиком, мог спокойно создавать новые протоколы и приложения, не опасаясь проблем внетехнического характера, то теперь ему, возможно, понадобится заручаться поддержкой отдельных провайдеров

интернет, чтобы быть уверенным, что его протокол будет работать как надо.

Потенциально, Comcast угрожает даже обычной конкуренции на рынке передовых услуг. Например, угрожая распространению онлайнового видео или создавая помехи раздаче трафика видеофайлов в P2P-сетях. Например, BitTorrent сейчас является официальным дистрибьютором ряда голливудских студий и, соответственно, прямым конкурентом для видеоуслуг от Comcast.

Остается разобраться с заявлением Comcast о суровой необходимости, заставляющей компанию применять активные средства управления сетью, во избежание проблем с передачей трафика, чувствительного ко времени задержки. Несмотря на слишком общую формулировку без каких-либо деталей, определенные выводы сделать можно.

Несомненно, что одни пользователи потребляют гораздо большие объемы трафика, чем другие, и что создание помех для пропускной способности их каналов может уменьшить в целом транспортные проблемы для оператора в целом. Но это вовсе не обозначает, что подделка пакетов становится правильным и законным средством регулирования - есть и другие механизмы, вполне законные и не влекущие за собой такого количества проблем.

Кроме того, во время тестирования не было замечено каких-либо изменений воздействий оператора в зависимости от объема трафика: закачивание файла объемом 500 Кб в один поток с узла BitTorrent немедленно привела к появлению RST-пакетов. Накануне по этому соединению связь вообще не устанавливалась, т.е. ранее это подключение не могло себя зарекомендовать в качестве "злостного качальщика". Система появление RST-пакетов не изменилась и на следующий день, когда через это соединение было принято около 500 Мб данных.

Если бы речь шла действительно об "управлении сетью", политика появления помех должна, по идее, варьироваться в зависимости от активности клиента: объема трафика или количества одновременно установленных сеансов связи.

При этом, существуют методики, вполне доступные для Comcast, позволяющие эффективно управлять полосой пропускания и без подделки пакетов. Например, можно воспользоваться технологиями динамического формирования потока трафика для конкретного пользователя. Можно установить предельный объем данных, который потребитель может получать/передавать за условную единицу времени. Можно сделать эти предельные объемы "плавающими", в зависимости от загруженности сети или активности пользователя.

Поскольку признаков динамического управления сетью на примере конкретного пользователя замечено не было, можно с определенной долей уверенности сказать, что Comcast, обратившись к регулированию своей сети через подделку пакетов, далеко не исчерпал все легальные (и абсолютно не сложные) возможности управления потоками данных в своей сети.

Вместе с тем, безотносительно к вариантам управления своими сетями, операторы должны предупреждать потребителей о возможных ограничениях, связанных с высокой активностью потребления трафика. Однако провайдеры интернет любят позиционировать свои услуги как "неограниченные" и без подсчета объемов трафика. Что не способствует хорошему отношению со стороны клиентов, не ожидающих проблем со связью, но сталкивающихся с ними ежедневно.

В принципе, конечные пользователи не совсем беззащитны перед произволом Comcast, хотя каких-либо доступных вариантов для персонального противодействия не так и много. Однако, все вместе, сообщество потребителей и программисты вполне в состоянии организовать эффективные контрмеры. Хотя, вероятно, ценой определенных затрат.

Одиночному пользователю трудно защититься от фальшивых RST-пакетов, поскольку они рассылаются и получателю, и отправителю трафика. Конечно, потребитель может попробовать настроить персональный брандмауэр на "вычисление" и фильтрацию фальшивок, но нет никаких гарантий, что на другой стороне соединения будут предприняты аналогичные действия. Кроме того, останется опасность блокировки вполне легальных RST-пакетов. Еще один вариант - использования криптографических методов защиты. Но и в этом случае, перед обменом данными требуется предварительная договоренность сторон.

Достойной альтернативой выглядит поиск протоколов, которые пока не подвергаются воздействию со стороны Comcast. К сожалению, этот вариант не гарантирует защиты надолго: в какой-то момент кабельный гигант может "добраться" до любого протокола.

Разработчики ПО имеют больше вариантов защиты от такого поведения провайдера и главный инструмент в их арсенале - это криптография. Внося изменения в программные продукты, программисты могут гарантировать применение одинаковых систем шифрования между незнакомыми друг с другом пользователями, и обеспечить проверку подлинности каждого пакета.

Практически, достижение подобных результатов может оказаться довольно дорогим

"удовольствием". Потребуются сложные схемы шифрования на разных уровнях для эффективной маскировки основного протокола, а также постоянный контроль за средствами обнаружения, используемые оператором для своевременного внесения необходимых изменений.

Остается надеяться, что подобное противостояние покажется руководству Comcast слишком затратным и малоэффективным, и провайдер откажется от подобных средств управления сетью.

Дмитрий